2013

A Video Steganography Attack Using Multi-Dimensional Discrete Spring Transform

Aaron T. Sharp
University of Nebraska-Lincoln, atsharp@huskers.unl.edu

Qilin Qi
University of Nebraska-Lincoln, qqi2@unl.edu

Yaoqing Lamar Yang
University of Nebraska-Lincoln, yyang3@unl.edu

Dongming Peng
University of Nebraska-Lincoln, dpeng2@unl.edu

Hamid Sharif
University of Nebraska-Lincoln, hsharif@unl.edu

A Video Steganography Attack Using Multi-Dimensional Discrete Spring Transform

Aaron Sharp, Qilin Qi, Yaoqing Yang, Dongming Peng, and Hamid Sharif

***Abstract*—Video steganography is fast emerging as a next-generation steganographic medium that offers many advantages over traditional steganographic cover media such as audio and images. Various schemes have recently emerged which take advantage of video specific properties for information hiding, most notably through the use of motion vectors. Although many steganographic schemes have been proposed which exploit several possible steganographic domains within video sequences, few attacks have been proposed to combat such schemes, and no current attacks have been shown to be capable of defeating multiple schemes at once.**

In this paper, we will further expand upon our proposed Discrete Spring Transform (DST) steganographic attack. We will explore further applications of the transform and how it may be used to defeat multiple steganographic schemes, specifically current video steganography schemes. The effectiveness of the proposed algorithm will be shown by attacking a multi-dimensional steganographic algorithm embedded in video sequences, where the scheme operates in two different dimensions of the video. The attack is successful in defeating multiple steganographic schemes verified by determining the BER after DST attack which always remains approximately 0.5. Furthermore, the attack preserves the integrity of the video sequence which is verified by determining the PSNR which always remains approximately above 30dB.

I. Introduction

Digital Steganography is often considered a game of cat and mouse between steganographer and attacker, where the two are constantly at odds attempting to defeat each other. In the last several decades, the capacity and prevalence of steganographic cover media has increased dramatically almost entirely as a direct result of the free exchange of media via the internet. Websites such as Facebook and Flickr are estimated to host approximately 100 billion and 6 billion images respectively [1] and Youtube is estimated to host approximately 13 billion videos [2]. As a result, steganographic attacks that can be applied to a variety of algorithms and cover media are becoming increasingly important since the sea of potential cover media is becoming so incredibly vast.

Although countless steganographic attacks have be proposed to combat a variety of steganographic algorithms [3], [4], [5], [6], very few attacks are flexible enough to be used outside of a limited set of algorithms and are typically highly-specialized to defeat certain types of steganographic algorithms. For example, we consider the attacks described [3], [4], [5], [6] which defeat image-steganography, and more specifically, jpeg-based steganography. None of the attacks found in these surveys indicate that they are capable of defeating other types of image-based steganography, such as spatial techniques, and even worse none of these attacks appear to be adaptable to other types of jpeg steganography. It follows that the rigidity of these attacks is due to the nature of the attack itself, where nearly all proposed attacks fall into the passive warden classification as described by the prisoner problem.

The prisoner problem is used to describe steganographic attacks where attacks fall into one of two categories: passive warden and active warden. The prisoner problem describes the process of two prisoners attempting to communicate secretly by sending hidden messages through a warden [7], [4], [3]. The warden's responsibility is to discover and/or destroy the hidden message. A passive warden attack describes the scenario where the warden monitors messages and only acts if the message appears to contain hidden data [4], [3]. Conversely, an active warden attack describes the scenario where the warden actively attempts to destroy or uncover the hidden data, regardless of the appearance of the message [4], [3].

The problem with passive warden attacks is that they are most often highly specific to a certain steganographic algorithms within a specific type of cover media [4], [3]. It is typically the case that such attacks look at certain attributes of the cover media to determine if a certain algorithm has been used or if the statistics of the cover media have been disturbed in a manner that suggests steganographic data is present [8], [9]. It is clear to see that such attacks would be ineffective against those algorithms or cover media which have not been fully studied, as it is impossible to predict attributes of unknown attacks. For this reason, we believe that the only truly adaptable steganographic attacks utilize the active warden model. We have previously described the Discrete Spring Transform (DST) which is an active warden attack that is capable of disrupting next-generation steganographic algorithms [10]. In this paper, we intend to further expand upon the DST attack and demonstrate how it may be further applied to other next-generation steganographic schemes.

The paper is described as follows: Previous Works, which briefly introduces the Discrete Spring Transform and Video Steganography; System Architecture and Methodology, which mathematically describes further applications of the Discrete Spring Transform and its applications; Video Steganography, which describes in detail the specifics of a multi-dimensional steganography scheme in video sequences; Simulation Results, which determines the results of the attack on video steganography; Conclusion, which describes the success of the attack and further observations.

Aaron T. Sharp, Qilin Qi, Yaoqing Yang, Dongming Peng, and Hamid Sharif are with the Department of Computer and Electronics Engineering, University of Nebraska, Lincoln, NE USA, Emails: {atsharp, qqi}@huskers.unl.edu, {yyang3, dpeng2, hsharif}@unl.edu

978-1-4799-0269-9/13/$31.00 ©2013 IEEE

II. Previous Works

Previous works for this paper focus on the discussion of Discrete Spring Transform (DST) and video steganograhy.

A. Discrete Spring Transform

We have previously described an active warden attack called the Discrete Spring Transform (DST) [10]. The attack utilizes spatial transforms to non-linearly distort cover media in a manner that destroys hidden steganographic data while preserving the integrity of the cover media. The definition of DST allows it to be applied to any type of stegranographic algorithm and cover media, which means that DST offers an extremely flexible and adaptable attack to combat next-generation steganography. It has been previously shown that DST may be applied to next-generation steganography (specifically to combat motion vector steganography) while preserving the integrity of the cover media. We intend to further expand the applications of DST to include a more generalized attack for video steganography.

B. Video Steganography

While video steganography is a relatively new steganographic medium, there have been some interesting schemes proposed which encode information in multiple domains of video sequences. Most of these techniques fall into one of three categories: 2-dimensional encoding, 3-dimensional encoding, and multi-dimensional encoding.

1) 2-Dimensional Video Steganography: 2-Dimensional video steganography refers to any techniques which may be used to encode information within individual frames of a video sequence using image-based steganography, example algorithms may be found in [11], [12], [13]. Since these techniques only operate 2-dimensionally within individual frames of the video sequence, the term 2-dimensional steganography is appropriate. There is nothing gained over image normal image-based steganography from using this technique as the strength of the algorithms are not enhanced when applied to video.

2) 3-Dimensional Video Steganography: 3-dimensional video steganography refers to techniques which attempt to encode information using a third dimension of the video sequence, such as time or motion vectors.

With time-based steganography, information may be spread in time by altering only certain frames, or sections of frames within a video sequence using image-based steganography. The advantage to this approach is that only a fraction of the possible frames and data are encoded, making steganographic attacks difficult since most of the video sequence will not contain any steganographic data. As a result, many steganographic attacks that take advantage of predefined statistics within image or video sequences would likely fail since the encoded video largely retains the same metrics as the original sequence.

Motion vector steganography encodes information within the motion vectors of a video sequence typically by intercepting the motion estimation block (as found in popular video compression algorithms) and altering motion vectors in a certain way [14], [15], [16], [17]. This technique utilizes motion between frames which is also considered a 3-dimensional medium for encoding. This attack is unique in that it takes advantage of a video-specific medium to encode information, meaning that image-based steganographic attacks are inadequate to defeat this type of steganography. Currently, the only observed attacks in literature are passive warden attacks that are specific to motion vector steganography [18], [19].

3) Multi-Dimensional Video Steganography: Multi-dimensional video steganography refers to a combination of 2-Dimensional and 3-Dimensional video steganography. Multi-dimensional steganography can simultaneously encode information in both the 3D and 2D sections of video, resulting in an extremely large capacity for steganographic data. In fact, often both techniques can be encoded independently of each other, meaning it is possible to encode two different sequences of information in two different domains of the video simultaneously. Figure 1 shows a block diagram of how 2D and 3D video steganography can both be applied to a video sequence. In this sample scheme, each frame of the video is encoded using standard image-based steganography (this frame is called the IFrame). Next, the next frame in the sequence (called the PFrame) is used to perform motion estimation from the IFrame. The PFrame is altered using motion-vector steganography to encode information. The cycle is then repeated by advancing the sequence using the PFrame as the new IFrame. The result of this type of encoding is that there is no current steganographic attack that can simultaneously address the 2D and 3D encoding in the video sequence. For this reason, we have chosen to attack multi-dimensional video steganography using our multi-dimensional DST to show how our attack can simultaneously defeat two different types of steganography schemes.

III. System Architecture and Methodology

We will now formally describe the definition of Discrete Spring Transform and some sample applications for specific types of cover media. The definition of the Discrete Spring Transform is independent of any specific steganographic algorithm and can be applied to any type of cover media in n-dimensional space.

A. Discrete Spring Transform

Let C be an n-dimensional cover media defined as:

$$C = F(x, y, z, \ldots) \tag{1}$$

where

$$x, y, z, \ldots \in Z \tag{2}$$

and the number of parameters in F(x, y, z, ...) is n.

Then the Discrete Spring Transform for a cover media C and attacked cover media $\hat{C}$ may be described as follows:

$$C = F(x, y, z, \ldots) \rightarrow AF(\lfloor ax \rfloor, \lfloor by \rfloor, \lfloor cz \rfloor, \ldots) = \hat{C} \tag{3}$$

978-1-4799-0269-9/13/$31.00 ©2013 IEEE

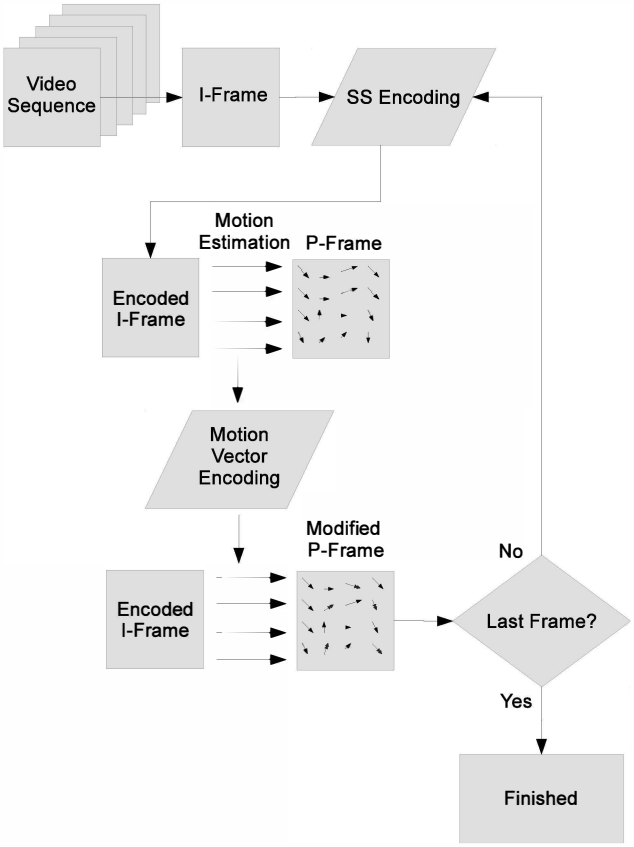

Fig. 1. Video Steganography Encoding

and A, a, b, c, ... ≈ 1 and are defined as:

$$\begin{aligned} A &= f_1(x, y, z, \ldots) \\ a &= f_2(x, y, z, \ldots) \\ b &= f_3(x, y, z, \ldots) \\ c &= f_4(x, y, z, \ldots) \\ \ldots &= f_n(x, y, z, \ldots) \end{aligned} \tag{4}$$

The strength of the Discrete Spring Transform lies in the definition of $f_n(x, y, z, \ldots)$, which we define as any non-linear and time-variant function. Unlike simple RST transforms, the non-linearity of the DST is applied to each dimension of the image.

B. DST for Image Media

Define an M x N pixel gray-scale image I as a cover media $I = F(x, y)$, where the number of pixels in x is M, and the number of pixels in y is N.

The DST is then realized as:

$$I = F(x, y) \rightarrow AF(\lfloor ax \rfloor, \lfloor by \rfloor) = \hat{I} \tag{5}$$

where A, a, b are defined as:

$$\begin{aligned} A &= f_1(x, y) \\ a &= f_2(x, y) \\ b &= f_3(x, y) \end{aligned} \tag{6}$$

and $f_n(x, y)$ is any non-linear time-variant function.

C. DST for Video Media

Define an M x N x F video (consisting of a sequence of F M x N gray-scale images) as a cover media $V = F(x, y, z)$, where the number of pixels in x is M, the number of pixels in y is N, and the number of frames is F.

The DST is then realized as:

$$V = F(x, y, z) \rightarrow AF(\lfloor ax \rfloor, \lfloor by \rfloor, \lfloor cz \rfloor) = \hat{V} \tag{7}$$

where A, a, b, c are defined as:

$$\begin{aligned} A &= f_1(x, y, z) \\ a &= f_2(x, y, z) \\ b &= f_3(x, y, z) \\ c &= f_4(x, y, z) \end{aligned} \tag{8}$$

and $f_n(x, y, z)$ is any non-linear time-variant function.

IV. Video Steganography Attack

As other steganographers have observed, video steganography is fast becoming an interesting new steganographic medium which has enormous capacity compared with traditional steganographic cover mediums [14], [15], [16], [17], [11]. For this reason, we have chosen to apply our multi-dimensional DST attack to video steganography. We have chosen to attack a scheme which encodes information in multiple steganographic domains of the video sequence, using image-based steganography and motion-vector steganography. Figure 1 describes the process of encoding information in the video sequence where information is encoded 2-dimensionally within individual frames of the video, as well as 3-dimensionally within the motion vectors of the video. We believe this scheme represents a robust system that would be exceptionally difficult to combat using existing steganographic attacks.

Our attack will utilize 2D and Time (3D) DST attacks to combat the multi-dimensional video steganography scheme. Figure 2 describes the process of attacking the video sequence as follows: First, the video sequence is decomposed into a train of 2D images or frames. Next each frame of the sequence is attacked using the 2D DST transform. Lastly, this resultant sequence is attacked using the Time (3D) DST attack. The semantics of the 2D and Time (3D) DST attacks are described in the following sections.

A. 2D DST Attack

The 2-dimensional DST attack has been previously described in [10], where the attack was applied to individual frames of a video sequence. The 2D DST attack can more generally be defined as an operation which will spatially distort media that can be expressed 2-dimensionally using a nonlinear spatial transform. Various algorithms may be applied which fit the criteria of a 2D DST attack, however, for simplicity we will focus on attacking the media using a 'pinch' attack, where individual sections of two-dimensional media are stretched and

978-1-4799-0269-9/13/$31.00 ©2013 IEEE

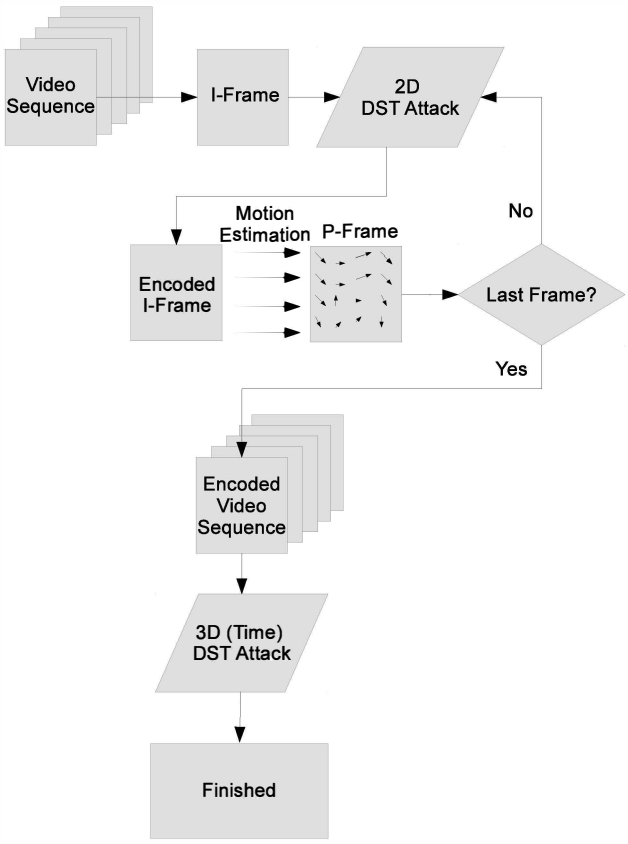

Fig. 2. DST Video Steganography Attack

other sections are compressed. The net effect of this nonlinear spatial attack is that the media retains some slight distortion but is effective in destroying most hidden steganographic data while maintaining an acceptable PSNR. This attack has been proven to be effective at combating complicated cover media such as video sequences, and will be part of the multi-dimensional Spring attack.

B. DST Time Attack

The DST Time attack is in principle identical to the 2D DST attack but is implemented in the third dimension of the steganographic media rather than the second dimension. It is understood that this attack can only be applied to those types of cover-media which exhibit at least three dimensions, such as video sequences. For a video sequence, this attack can be thought of as affecting the time or framerate, hence the title DST Time attack. Figure 3 describes the process of a simple DST Time attack, where a video sequence is first arbitrarily split into two video sequences. Next, each of these sequences is stretched or compressed via 3-dimensional interpolation in the time dimension. The result is that the number of frames in one sequence is decreased while the number of frames in the other sequence is increased. The resulting sequences are then combined to form a video sequence that has the same number of frames as the original sequence. This attack will be applied as part of the multi-dimensional Spring attack.

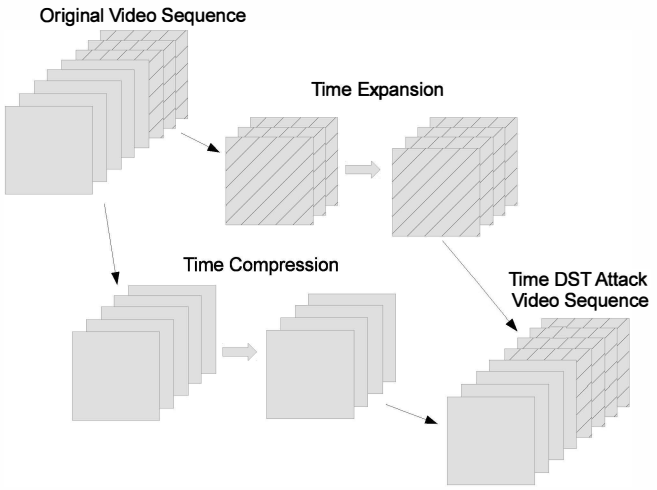

Fig. 3. DST Time Attack

V. Simulation Results

The results of our multi-dimensional DST attack indicate that our attack is successful in destroying the hidden steganographic data while maintaining acceptable quality of the cover-media. The BER for both the 2D and motion vector steganography schemes were calculated separately according to the strength of the 2D and Time DST attack.

A. 2D DST BER

Table I shows the BER for the 2D steganographic scheme under the multi-dimensional DST attack. As evident, the BER of the 2D steganographic scheme was increased dramatically with the 2D and Time DST attack. The table indicates that the 2D DST attack was much more successful in destroying the steganographic media than was the Time DST attack, however, even for a modest 2D DST attack the BER increases to approximately 0.5 which is shown in highlight.

		2D Chop (pixels)					
		0	10	20	30	40	50
Time Chop (frames)	0	0.0003	0.1020	0.5351	0.5195	0.5185	0.4611
	5	0.0006	0.1033	0.5364	0.5214	0.5077	0.4531
	10	0.0010	0.1043	0.5418	0.5236	0.5086	0.4557
	15	0.0010	0.1052	0.5402	0.5293	0.5140	0.4534
	20	0.0010	0.1043	0.5450	0.5332	0.5057	0.4544
	25	0.0013	0.1087	0.5421	0.5360	0.5061	0.4585

TABLE I
2D Steganography BER

B. Time (3D) DST BER

Table II shows the BER for the motion vector scheme under the multi-dimensional DST attack. It can be seen that the BER of the 3D steganographic scheme was increased significantly under either the 2D or Time DST attack. Unlike the 2D steganographic scheme, both the 2D and Time DST attacks were equally successful in combating the motion vector steganography, as evidenced by the fact both schemes successfully increase the BER to 0.5 dB.

978-1-4799-0269-9/13/$31.00 ©2013 IEEE

Time Chop (frames)	2D Chop (pixels) 0	10	20	30	40	50
0	0.0000	0.0000	0.3891	0.4713	0.5161	0.5146
5	0.5197	0.5257	0.5106	0.5338	0.4970	0.5015
10	0.5423	0.5302	0.5474	0.4945	0.5121	0.5287
15	0.4990	0.5318	0.5484	0.5378	0.5484	0.5237
20	0.5302	0.5635	0.5181	0.5297	0.5297	0.5156
25	0.5514	0.5559	0.5413	0.5398	0.4950	0.5186

TABLE II
MOTION VECTOR STEGANOGRAPHY BER

C. Cover Media Quality

Table III shows the PSNR for the video sequence under the multi-dimensional DST attack. The results indicate that the PSNR was acceptable for all tested DST transforms, where the PSNR always remains close to 30dB. The optimal transform widths for these schemes were indicated by the shaded cell in each of the three tables, where the 2D DST Chop was 20 pixels and the Time (3D) DST Chop was 10 frames.

Time Chop (frames)	2D Chop (pixels) 0	10	20	30	40	50
0	∞	30.887	29.686	29.339	29.144	29.018
5	34.250	30.136	29.377	29.137	28.994	28.898
10	32.238	29.765	29.223	29.036	28.913	28.828
15	31.470	29.594	29.141	28.979	28.868	28.792
20	31.090	29.496	29.092	28.943	28.838	28.769
25	30.864	29.435	29.059	28.919	28.817	28.752

TABLE III
MOTION VECTOR STEGANOGRAPHY PSNR (DB)

VI. CONCLUSION

In this paper, we have presented a novel new active warden steganographic attack called multi-dimensional Discrete Spring Transform that is capable of simultaneously defeating multiple types of steganographic schemes. We have shown how the attack can successfully be applied to video steganography where information is encoded in multiple domains of the video. The results of the attack indicate that the BER of both steganographic schemes is increased to approximately 0.5 for even a modest DST transform, results also indicate that the quality of the cover media is acceptable for all simulated DST where the PSNR remains close to 30dB for all cases.

We would like to reiterate that the strength of the DST attack remains in its ease of implementation and the fact that it can simultaneously defeat multiple types of steganography without significantly impacting the quality of the cover media. As steganographic schemes continue to increase in their sophistication the need for strong yet flexible attacks becomes a necessity where the DST presents a viable solution.

ACKNOWLEDGEMENT

This paper was funded in part by the Nebraska Research Initiative on Multimedia Rendering.

REFERENCES

[1] Pingdom. (2012, jan.) Internet 2011 in numbers. [Online]. Available: http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/

[2] C. Rick. (2010, apr.) 13 billion videos on youtube for 135.7 million viewers in april. [Online]. Available: http://www.reelseo.com/13-billion-videos-april/

[3] M. Kharrazi, H. T. Sencar, and N. Memon, "Image steganography: Concepts and practice," *Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore*, 2004.

[4] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and image steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, 2011.

[5] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062 –1078, jul 1999.

[6] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064 –1087, jun 1998.

[7] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *CRYPTO*, 1983, pp. 51–67.

[8] N. Provos and P. Honeyman, "Detecting steganographic content on the internet," In ISOC NDSS02, Tech. Rep., 2001.

[9] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems - breaking the steganographic utilities ezstego," in *Jsteg, Steganos, and S-Tools - and Some Lessons Learned, Lecture Notes in Computer Science*. Springer-Verlag, 2000, pp. 61–75.

[10] A. Sharp, Q. Qi, Y. Yang, D. Peng, and H. Sharif, "A novel active warden steganographic attack for next-generation steganography," *International Wireless Communications and Mobile Computing Conference*, July 2013.

[11] S. Hu and U. KinTak, "A novel video steganography based on non-uniform rectangular partition," in *Computational Science and Engineering (CSE), 2011 IEEE 14th International Conference on*, aug. 2011, pp. 57 –61.

[12] B. Liu, F. Liu, C. Yang, and Y. Sun, "Secure steganography in compressed video bitstreams," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, march 2008, pp. 1382 – 1387.

[13] K. Raghavendra and K. Chetan, "A blind and robust watermarking scheme with scrambled watermark for video authentication," in *Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on*, dec. 2009, pp. 1 –6.

[14] A. Sharp, J. Devaney, and A. Steiner, "Digital video authentication with motion vector watermarking," in *Signal Processing and Communication Systems (ICSPCS), 2010 4th International Conference on*, dec. 2010, pp. 1 –4.

[15] N. Mohaghegh and O. Fatemi, "H.264 copyright protection with motion vector watermarking," in *Audio, Language and Image Processing, 2008. ICALIP 2008. International Conference on*, july 2008, pp. 1384 –1389.

[16] Z. Liu, H. Liang, X. Niu, and YixianYang, "A robust video watermarking in motion vectors," in *Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on*, vol. 3, aug.-4 sept. 2004, pp. 2358 – 2361 vol.3.

[17] A. Ceddillo-Hernandez, M. Nakano-Miyatake, L. Rojas-Cardenas, and H. Perez-Meana, "Robust video watermarking using perceptual information and motion vector," in *Circuits and Systems, 2007. NEWCAS 2007. IEEE Northeast Workshop on*, aug. 2007, pp. 811 –814.

[18] C. Zhang, Y. Su, and C. Zhang, "A new video steganalysis algorithm against motion vector steganography," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, oct. 2008, pp. 1 –4.

[19] Y. Su, C. Zhang, and C. Zhang, "A video steganalytic algorithm against motion-vector-based steganography," *Signal Process.*, vol. 91, no. 8, pp. 1901–1909, Aug. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.sigpro.2011.02.012

978-1-4799-0269-9/13/$31.00 ©2013 IEEE